IT security policy for HSR Users

IT Services provide the members of HSR Hochschule für Technik Rapperswil with a stable IT environment. Every user is responsible for the security of the data processed during his/her field of use. To ensure optimum information security on the devices used, the users must adhere to the prescribed security policy.

1 Scope

- These information security policies apply to all members of HSR as well as to third parties. By third parties is meant all users who use the IT resources and/or have an account (user account) at HSR.
- Considered as members of HSR are all lecturers, students and employees of HSR.
- By the term Use or Exploitation is meant any type of electronic processing of data by means of devices or services.
- The binding and most up-to-date version of the Rules of Use can be found on http://www.hsr.ch – HSR-Intern – IT-Sicherheit und Datenschutz – IT-Sicherheit – Kontakt & Dokumente

2 Use of the IT workrooms and IT resources

- Devices and supporting documents installed in the IT workrooms must not be removed from these rooms.
- Carrying out any modifications to the devices (hardware and software) is strictly prohibited.
- Bundling processing power (multiple logins, cluster mechanisms) is only permitted under the supervision of a teacher and with the consent of the IT Services.
- IT resources on loan must be returned on time.
- No private, commercial use or use against payment of HSR IT resources is allowed unless it has been expressly approved.
- In the IT workrooms, the general HSR university rules (no smoking, eating or drinking) and the additional regulations posted up apply.

3 Protection of terminals and passwords

- The PCs must not be used without authorization in the absence of users. Therefore, if the workstation is vacated, the PC must be locked.
- To protect the programs and data, the IT Services give all users a user name with password. This password must be changed after the first login.
- The password is strictly confidential and must not be disclosed. Users may be held responsible if unauthorized access to data is made using their password.
- Users are responsible for the administration of their password.
- The password must be chosen according to the guidelines of the HSR password policy and changed regularly.
- Trying out, researching and using third-party access authorizations (e.g. login, passwords, personal identifications etc.) and other authentication aids (e.g. chip cards, magnetic cards, etc.) are prohibited.

4 Handling data and programs

- The responsibility for the stored data lies fully with the users.
- Any abusive acquisition of data and programs is prohibited.
- Any abusive use, modification or deletion of third parties' data is prohibited.
- Text, image and sound documents not in the interests of HSR must not be used or processed at HSR or stored on HSR IT systems.
- Data not stored on the central data storage system is not secured by the IT Services. The user is responsible him/herself for the security of this data.
- Running, installing or making available computer games of any sort is prohibited in the IT rooms. Likewise all network games via the network are prohibited.

5 Handling sensitive data

Sensitive data includes personal data as laid down in the Data Protection Act as well as all confidential data from teaching, research and administration. For handling sensitive data, the guidelines and classification of HSR for data privacy and protection of information apply. These can be viewed on the Intranet in the “Data Privacy” area on http://www.hsr.ch – HSR-Intern – IT-Sicherheit und Datenschutz – Datenschutz – Dokumente.
The following in particular applies:

- Sensitive data may only be viewed and processed by authorized persons. They are responsible for ensuring that such data is only stored in the designated data storage and are viewed and processed with the designated means of access. They are likewise responsible for ensuring that unauthorized persons may not obtain access to sensitive data via their means of access.
- Data collections of personal data must be reported to the data protection officer.
- Sensitive data on mobile devices must be stored encrypted. HSR notebooks are mandatorily set up with disk encryption.
- Sensitive data transmitted electronically must be encrypted. Transmitting sensitive data abroad is not allowed.
- When a person leaves HSR, sensitive data must be handed over unencrypted to any successor and must not be taken away with him/her.
- Data carriers with sensitive data must be destroyed on disposal.
- Sensitive data must not be stored outside the HSR infrastructure. HSR assumes no liability for data stored externally (e.g. in the cloud).
- The processing of sensitive data by third parties must follow the applicable guidelines. Confidential data must only be disclosed in anonymized form or encrypted with a corresponding confidentiality statement.

6 Connection and Use of HSR Network

- Using a mobile device as a gateway to the internet while it is connected with the PC is not permitted. This method enables direct access to the HSR network by bypassing all security mechanisms.
- The prescribed network security mechanisms (firewalls) must not be bypassed. The use of own VPNs to access HSR devices externally is not permitted.

7 Use of Internet Services

- The use of internet services must have a connection with the HSR assignment, i.e. teaching, further training or research.
- It is not permitted to access websites with:
  - erotic, pornographic or sexual content
  - racist or violent content
  - content that is contrary to accepted principles of morality in any other way.
- The use of internet services for private purposes is in principle prohibited. For short activities that only place a minimal demand (e.g. SBB timetable) on the internet access, the internet access may be used for private purposes.
- Downloads and uploads for private purposes (e.g. MP3, images etc.), listening to music, watching films and TV programs via the internet are not allowed.
- The use of software for exchanging data such as music or films is prohibited.
- On devices not installed by the IT Services, the virus scanner is to be installed in such a way that downloads are automatically scanned for viruses.

8 Use of Email Services

- Using HSR email services is prohibited for:
  - spam emails
  - political purposes
  - private advertising purposes
  - emails with illegal content
- The HSR email address may only be used in connection with the assignment at HSR.
- The private use of the email services is to be exercised sparingly.

- Email distribution lists (e.g. pers.all, stud.all) may only be used by senior HSR managers (e.g. Head of School, Head of Study Course) or with their permission.
- Automatically forwarding emails to private or other external mailboxes is prohibited. For permanent access to the HSR mailbox, WEB Mail or Outlook Anywhere must be used.
- On devices not installed by the IT Services, the virus scanner is to be installed in such a way that attachments are automatically scanned for viruses on opening.
- Suspicious emails must be deleted unread from the inbox. Caution is to be exercised in the case of unusual subject lines even if the emails come from known senders.
- Confidential information must not be sent unprotected and unencrypted as an email.

9 Anti-virus and Personal Firewall

- The anti-virus program and the virus signature file of HSR computers is periodically replaced by a new version so that new virus types can also be recognized. It is forbidden to switch off the anti-virus programs on the HSR devices.
- The personal firewall (Windows firewall) is switched on by default on the HSR devices. It is prohibited to switch off or bypass the firewall.

10 Use of Mobile Devices

Mobile devices (notebooks, tablets, smartphones etc.) and removable drives (USB sticks, memory cards, CDs/DVDs etc.) can in principle be used if the following general conditions are met.

- Users who use their private mobile devices at HSR are themselves responsible for the operation and licensing of the software installed on them.
- If a mobile device is connected with the HSR network, it is mandatory to use a functional and activated virus scanner. There is a virus scanner available on: http://www.hsr.ch – HSR-Intern – Informatikdienste – Persönliches Notebook- Sicherheit, Virenschutz und Datensicherung.
- To gain access to the HSR network with mobile computers, the use of a personal firewall is absolutely essential.
- Mobile devices must be secured with a startup password, USB sticks should be password-protected and the data encrypted.
- Without special approval, all IT resources paid for by HSR are to be procured via the central purchasing office of the IT Services. Standards are specified.

11 Clear Desk Policy

When the workstation is vacated, the workstation is to be properly tidied. This means:

- Confidential documents in printed form must be locked in the appropriate filing cabinets or in the desk.
- Confidential documents no longer needed must be destroyed (document shredder) or disposed of in the containers for that purpose. They must not be put in the recycle bin.
- If the workstation is vacated, even if only for a short time, the computer must be locked with password protection.
- In the case of longer absence and overnight, the computer must be shut down properly.
- The windows and doors must be closed.
- The office door must be locked if possible.
- Doors to side rooms with confidential data or valuable content must be locked.

12 Copyright and Use

- Copying or referencing text, image and sound documents without the written consent of the responsible body of authors and license rights is not permitted.
- The rights to programs, software, text, image and sound documents which arise in projects of the institution with industry are to be laid down in special contracts by those with appropriate responsibility. The responsibility for compliance with the license terms lies with the project leader.
- All programs, software, text, image and sound documents developed otherwise by members and students at HSR can be freely used by members of HSR without licenses and fees.

13 Abuse, Controls and Sanctions

- The following are considered as abuse:
  - Violating the present regulations
  - Violating higher-level law
  - Violating license rights
  - Violating data protection
  - Copyright infringement
  - Disproportionate or unapproved use of the IT resources
  - Storing, printing, sending or displaying data that is incompatible with the task and reputation of HSR, in particular data with a racist, extreme right-wing, sexist or pornographic content
  - Infringing, disrupting or impairing internal or third-party infrastructure (email, web or network services).
  - Bullying, violation of the personal rights or reputational damage of third parties
- The IT Services monitor the technical resources in the form of automated logging (virus scanner, memory usage, network monitoring etc.)
- If there is suspicion of abuse, the IT security officer, in consultation with his superior, is authorized to secure data for evidence purposes.
- If abuse is present, the IT security officer, in consultation with his superior, is authorized to block access to IT resources or delete data.
- On the request of the IT security officer, the HSR school management will decide on the initiation of a disciplinary or criminal proceedings.
- Costs that HSR incurs in connection with abuse will be charged to the perpetrator. If there is breach of copyright, HSR will refuse to accept any responsibility and liability. The perpetrator is him/herself liable for the consequences.

14 High-level law

The present provisions are based primarily on the Swiss federal laws on copyright and data protection and the corresponding laws of the Canton of St. Gallen as well as on the contractual agreements that HSR and its associated groups have concluded on licenses and services of any sort. The authoritative legal regulations, alongside the license agreements, ZGB (Swiss Civil Code) and OR (Swiss Code of Obligations), are the following statutory provisions:

- DSG Data Protection Act
- VDSG Data Protection Regulations
- FMG Telecommunications Act
- PatG Patent Act
- URG Copyright Act
- URV Copyright Regulations

15 Further information

Additional information for handling IT resources and on IT security and data protection can be found on:

- http://www.hsr.ch – HSR-Intern – Informatikdienste
- http://www.hsr.ch – HSR-Intern – IT-Sicherheit und Datenschutz

Rapperswil, 7 September 2015
HSR Hochschule für Technik Rapperswil
Administrative Director
IT Security and Data Protection